Site Security Certification Report

SCO Operation Site

Sponsor and developer: ***Sony Corporation***
Sony City Osaki 24th floor, 2-10-1 Osaki, Shinagawa-ku,
Tokyo, 141-8610
Japan

Evaluation facility: ***Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-SS-0330424-CR**

Report version: **1**

Project number: 0330424

Author(s): **Brian Smithson**

Date: **14 July 2021**

Number of pages: **9**

Number of appendices: **0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

At the time of publication, the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) do not cover the recognition of Site Certificates. The site-security evaluation process, however, followed all the rules of these agreements and used the agreed supporting document for site certification *[CCDB]*. Therefore, the results of this evaluation and certification procedure can be reused by any scheme in subsequent product evaluations and certification procedures that make use of the certified site.

Presence of the CCRA and SOG-IS logos on this certificate would indicate that the certificate is issued in accordance with the provisions of the CCRA and the SOG-IS MRA and is recognised by the participating nations. The CCRA and the SOG-IS MRA do not cover site certification, however, so these logos are not present on this certificate.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SCO Operation Site. The operator of the site is Sony Corporation located in Tokyo, Japan and they also act as the sponsor of the evaluation and certification.

The evaluated site is: SCO Operation Site, located on the 24th floor of the Sony City Osaki building, which is fully occupied by Sony.

The site is used by FeliCa Business Division to participate in the activities of IC Embedded Software Development, Test Program Development, Verification and Validation (Phase 1). To perform its activities the site uses corporate IT infrastructures and dedicated services, implemented in an on-site secure data center, according to Sony defined processes. The site activities are related to Phase 1 of the seven Phases of the Lifecycle Model as defined in [PP].

The site has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 14 July 2021 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the Site Security Target *[SST]*, which identifies assumptions made during the evaluation and the level of confidence (evaluation assurance level) the site is intended to satisfy for product evaluations. Users of this site certification are advised to verify that their own use of, and interaction with, the site is consistent with the Site Security Target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report *[ETR]*[1] for this site provide sufficient evidence that this site meets the EAL6 assurance components: ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2 at AVA_VAN.5 level, ALC_LCD.1, and ALC_TAT.3.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* and the Supporting Document Guidance: CCDB-2007-11-001 Site Certification, October 2007, Version 1.0, Revision 1 *[CCDB]*, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the site certificate will be included on the NSCIB Certificates list. Note that the certification results apply only to the specific site, used in the manner defined in the *[SST].*

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Site Identification

The Target of Evaluation (TOE) for this evaluation is the SCO Operation Site located in Tokyo, Japan.

2.2 Scope: Physical

This site certification is located on 24th floor of Sony City Osaki, a building which Sony fully occupies. The whole building is security-controlled by Sony. Relevant activities take place is limited to two secured areas: the development area, and the server room. Only authorised persons including subcontractor are allowed entry to the development area. Further restrictions to access apply to the server room.

2.3 Scope: Logical

The site is used by FeliCa Business Division to perform the development and testing of the embedded software for security ICs. The development server, the dedicated network with the firewall, and local IT equipment, are located within the site. The developer can access the dedicated network remotely through VPN gateway server that FeliCa Business Division provides and manages. The configuration management is provided by the configuration management tool in the development server.

The activities in the site is Security IC Embedded Software Development (Phase 1) as defined in the Protection Profile *[PP]*. Within those phases, the site is involved in:

- ALC_DVS to control access to the assets (at AVA_VAN.5 level).
- ALC_CMC/CMS to handle the site internal documentation and TOE development related configuration items.
- ALC_LCD as part of TOE development and testing.
- ALC_TAT as part of TOE development and testing.
- ALC_DEL to maintain security of TOE delivery.

2.4 Evaluation Approach

The evaluation is a first evaluation.

In the evaluation all evaluator actions have been performed including a site visit that was performed in accordance with the temporary SOGIS policy *[JIL-CovPanPol]* as a “virtual audit”. Previously the site was physically audited in 2019 during a product certification CC-20-214607 *[CR-214607]*. For assessment of the ALC_DVS aspects, the Minimum Site Security Requirements *[MSSR]* have been used.

2.5 Evaluation Results

The evaluation lab documented its evaluation results in the *[ETR]*[2], which references other evaluator documents. To support reuse of the site evaluation activities a derived document *[STAR]*[3] was provided and approved. This document provides details of the site evaluation that must be considered when this site is used in a product evaluation.

The evaluation lab concluded that the site meets the assurance requirements listed in the *[SST]* as assessed in accordance with *[CC], [CEM]* and *[CCDB]*.

---

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

[3] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

2.6 Comments/Recommendations

The Site Security Target *[SST]* contains necessary information about the usage of the site. During a product evaluation, the evidence for fulfilment of the Assumptions listed in the *[SST]* shall be examined by the evaluator of the product when reusing the results of this site evaluation.

3 Site Security Target

The Site Security Target for SCO Operation Site, SCO-SST-E00-11, Rev. 0.11, November 2020 *[SST]* is included here by reference.

Please note that for the need of a public version, *[SST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MSSR	Minimum Site Security Requirements
NSCIB	Netherlands Scheme for Certification in the area of IT Security
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CCDB]	Supporting Document Guidance: CCDB-2007-11-001 Site Certification, October 2007, Version 1.0, Revision 1
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[CR-214607]	Certification Report RC-SA20,RC-SA21 and RC-SA24 Series version 1.00, report version 1.0, 05 June 2020
[ETR]	Evaluation Technical Report Site Security SCO Operation Site, 21-RPT-202, version 3.0, 14 July 2021
[JIL-CovPanPol]	JIL Temporary Covid19 pandemic operational SOGIS evaluation and certification policy and rules, Version 1.2, June 2021
[MSSR]	Joint Interpretation Library, Minimum Site Security Requirements, Version 3.0, February 2020
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP]	Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Revision 1.0, 13 January 2014
[SST]	Site Security Target for SCO Operation Site, SCO-SST-E00-11, Rev. 0.11, November 2020
[SST-lite]	Site Security Target for SCO Operation Site, SCO-SSTP-E01-00, Rev. 1.00, June 2021
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR]	Site Technical Audit Report – Sony SCO Operation Site, 21-RPT-203, version 3.0, 14 July 2021

(This is the end of this report.)